IN THE CLAIMS

Please amend Claims 1 - 3 and 11 as follows:

1. (*Currently amended*) A method of authenticating a transaction, <u>the method</u> comprising:

    ~~connecting~~ <u>causing</u> a separate unit to <u>communicate with</u> a device ~~having a keypad and display~~, the separate unit being secured and independently operating from the device<u>, the separate unit configurable to include a first biometric sensor to obtain first biometric characteristics of a user, the first biometric characteristics physically representing the user</u>;

    initiating a transaction request using the device;

    communicating the transaction request to a third party through the device; and

    receiving a signal at the separate unit via the device to authenticate the transaction, wherein the separate unit is caused to request personalized data from ~~a~~ <u>the</u> user associated with the device, the separate unit is not to encrypt the transaction but to authenticate the transaction between the device and the third party <u>only when the biometric characteristics of the user is verified</u>, the transaction can only be authenticated when the personalized data is authenticated in the separate unit.

2. (*Currently amended*) The method of claim 1, wherein the separate unit is ~~a portable card reader unit is capable of reading a smartcard~~ <u>further configurable to include a second biometric sensor to acquire second biometric characteristics of the user to ensure that the user is indeed authenticated</u>.

3. (*Currently amended*) The method of claim 1, wherein ~~the separate unit is a portable card reader unit is capable of reading an optical card~~ <u>the first biometric sensor is a fingerprint sensor to acquire a fingerprint of the user, and the second biometric sensor is a microphone to acquire a voice of the user</u>.

4. (*Original*) The method of claim 1, wherein the device is a personal digital assistant (PDA).

5. (*Original*) The method of claim 1, wherein the device is a telephone.

6. (*Original*) The method of claim 5, wherein the telephone is a cellular telephone.

7. (*Original*) The method of claim 1, wherein the signal used to authenticate the transaction is a high-contrast optical signal.

8. (*Previously amended*) The method of claim 1, wherein said communicating the transaction request to the third party involves a use of a dual-tone audio signal.

9. (*Original*) The method of claim 8, wherein the signal is a dual-tone, multi-format (DTMF) signal.

10. (*Original*) The method of claim 8, wherein the signal is an audio frequency shift keying (AFSK) signal.

11. (*Currently amended*) The method of claim 8, wherein the signal is a private line (PL) signal or a wireless signal.

12. (*Previously amended*) The method of claim 1, wherein said initiating a transaction request includes an entry of a personal identification number (PIN) through the keyboard of the device.

13. (*Previously amended*) The method of claim 12, wherein the separate unit is terminated if a PIN entry is attempted more than a predetermined number of times.

14. (*Previously amended*) The method of claim 1, wherein the separate unit further includes a biometric input; and said initiating a transaction request includes receiving biometric data through the biometric input.

15. (*Original*) The method of claim 14, wherein the biometric input is a fingerprint.

16. (*Previously amended*) The method of claim 1, wherein one or both of the transaction request and the authentication signal are encrypted.

17. (*Original*) The method of claim 16, wherein the encryption is based on public-key cryptography.

18. (*Previously amended*) The method of claim 1, wherein the separate unit or device includes a memory; the transaction request and authentication signal constitute a session; and information regarding the session is stored in the memory.

19. (*Previously added*) The method of claim 1, wherein the separate unit is a headset.

20. (*Previously added*) The method of claim 19, wherein the headset includes capability of reading in confidential information from a user associated with the device.